Hp Compaq t5000 Thin Clients

August 2004

invent

Instructions

Thin Client Virus Vulnerability Analysis

HP Compaq t5000 Thin Clients

Table Of Contents

Table Of Contents 1
Executive Summary 2
Virus Vulnerabilities, Encounters and Impact 3
Virus Encounter Vectors 3
Impact of Client Computing Vulnerabilities 4
HP Thin Client Response to Vulnerabilities 5
Thin Client Firewall 8
Recovery Time 8
Summary 9

Executive Summary

Enterprise computing networks require effective protection against computer viruses and other security issues. These security breaches can result in costly service calls, user downtime and loss of business-critical data. When compared to the traditional unmanaged PC network model, the HP thin client computing model yields a less vulnerable segregated approach to computing with substantially better recovery time, while minimizing total cost of ownership (TCO).

According to an ICSA Labs virus analysis[1], the average downtime lost during an encounter was 23 person days. This down time accounted for data loss recovery and patching the connected network servers and PCs. With the HP thin client computing model, your exposure to virus attack on the thin client system is over 80% less than a standard Windows PC. This means that your user will experience significantly less downtime due to security vulnerabilities than a PC user. In addition, since no user data resides on the thin client, there is no risk of user data loss on the thin client. Finally, if a thin client's image is compromised or corrupted , the recovery time is typically measured in minutes instead of hours.

Furthermore, the HP thin client computing model utilizes PC blades and/or servers located in the data center. These centralized devices can be protected and monitored more easily with centrally managed virus and firewall tools. Compromised resources can be quickly taken offline, corrected, or recovered faster and cheaper than distributed PC resources.

This model also allows a user's data to be segregated and centralized for easy backup and recovery, ensuring a higher level of service and security for your users at a lower TCO than distributed PC resources.

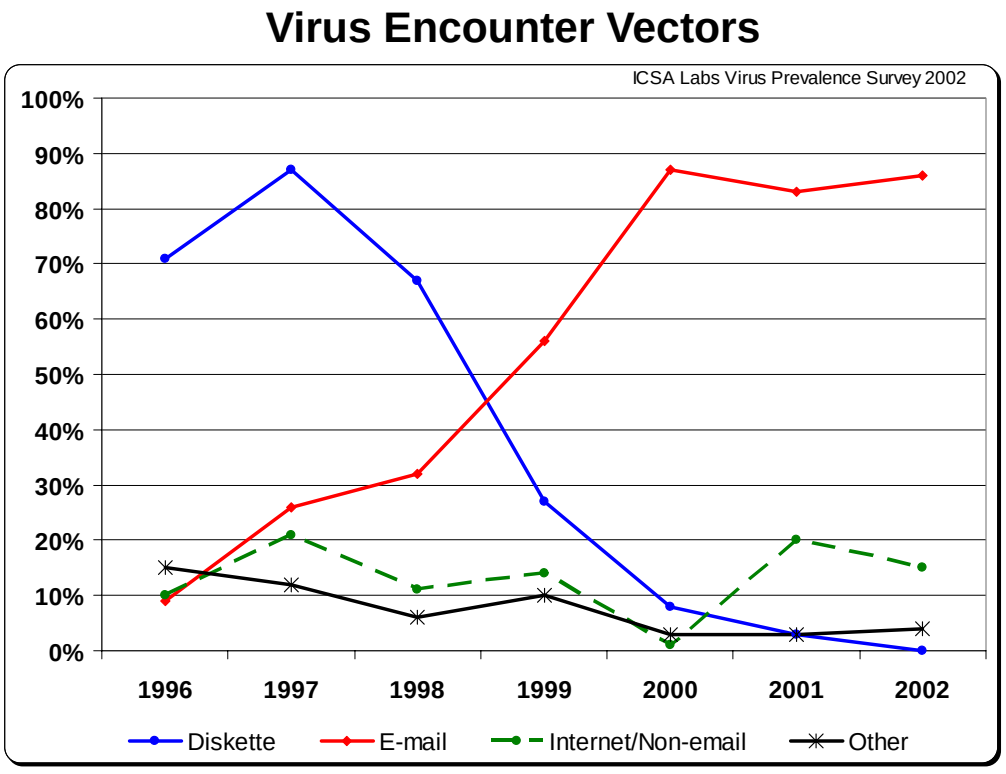
At HP, we realize security and TCO are important factors in enterprise computing. A Fall 2003 EDC survey showed more than eight out of every 10 enterprises suffered a security breach as a result of malicious code. As a result, more than half the enterprises are increasing their IT security budgets. HP believes the thin client computing model is an effective solution for the security conscious enterprise.

[1] *ICSA Labs 8th Annual Computer Virus Prevalence Survey*

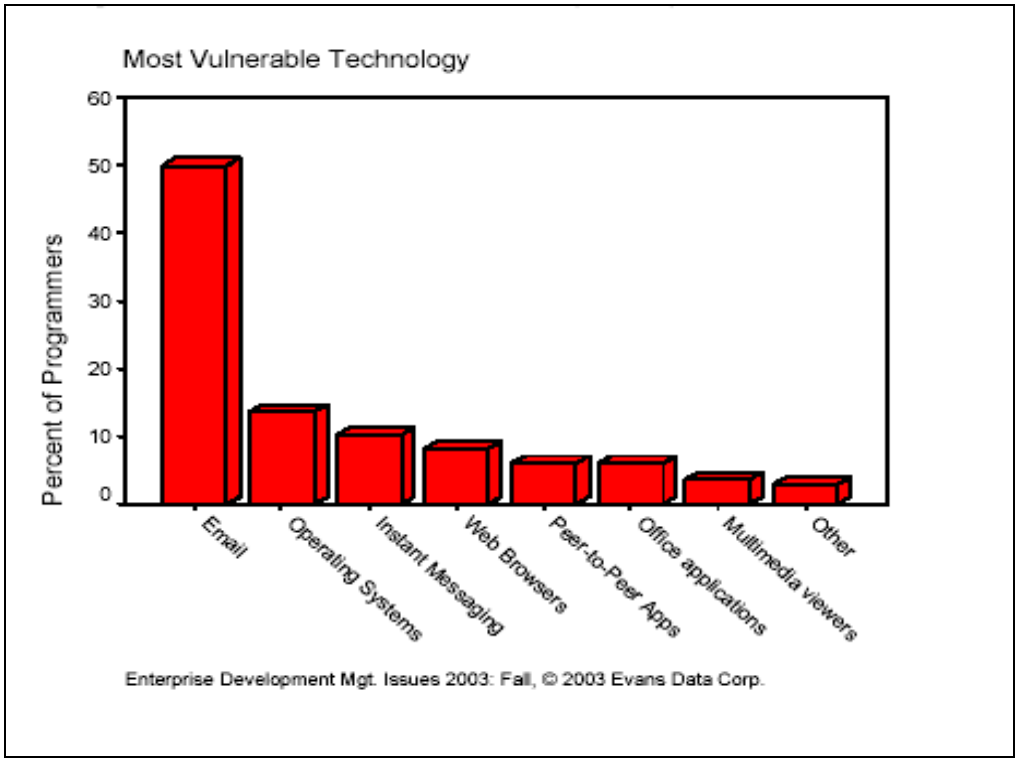
Virus Vulnerabilities, Encounters and Impact

The following graph depicts security vulnerabilities experienced by actual enterprise customers as surveyed by ICSA Labs for the years 1996 through 2002. The second graph contains the most vulnerable technologies as perceived by the enterprises surveyed in 2003 by EDC. The graphs illustrate a strong correlation between the actual occurrence of each vulnerability and its associated technology in an enterprise. For example, 86% of the encounters experienced in 2002 were email related and according to EDC, 50% of the enterprises surveyed in 2003 perceive email as their most vulnerable technology.

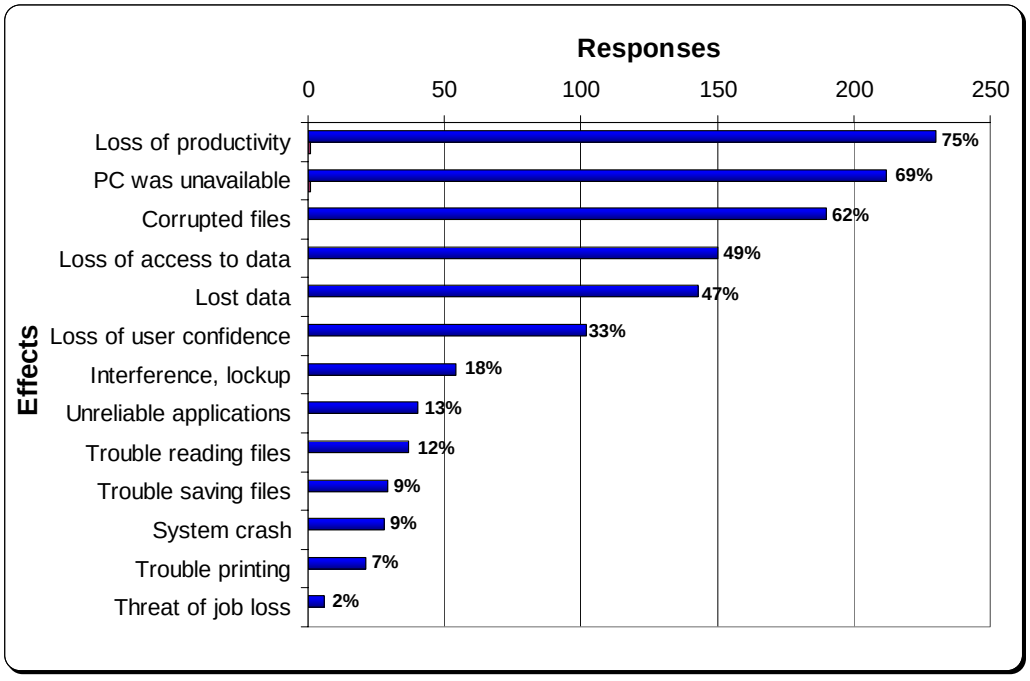
The third graph illustrates the impact of these vulnerabilities on the enterprises surveyed by ICSA in 2002.



Note: Other in this graph represents unknown vectors and 3rd party/freeware software distribution



Impact of Client Computing Vulnerabilities



ICSA Labs Virus Prevalence Survey 2002

HP Thin Client Response to Vulnerabilities

Given the data in the previous section, the thin client computing model substantially reduces the likelihood that the client device will encounter a vulnerability as compared to a standard PC. It also centralizes an enterprise's most vulnerable technologies in the data center where they can be most effectively controlled and protected from exposure at the user level.

The following table summarizes the previous data and shows that thin clients are substantially less susceptible to the virus vectors and are exposed to fewer of the perceived vulnerable technologies than a standard PC. The following sections detail these areas as related to the thin client computing model.

Technology	Personal Computers (PC)		Thin Client (TC)	
	2002 Encounter Vector Experienced[2]	2003 Perceived Vulnerability[3]	2002 Encounter Vector Experienced[2]	2003 Perceived Vulnerability[3]
Email	86%	49.9%	0%	0%
Operating System	0%	13.5%	0%	13.5%
Instant Messaging	0%	10.1%	0%[4]	0%[4]
Web Browser	4%	8.1%	0%[4]	0%[4]
Peer-to-Peer Apps	11%	6%	0%	0%
Office Applications	0%	6%	0%	0%
Multimedia Viewers	0%	3.6%	0%4	0%[4]
Other[5]	4%	2.9%	0%	0%
Total	105%	100%	0%	13.5%

Diskette/Removable Media

The intrusion of viruses from diskettes has declined significantly over the years and does not appear to be a significant vulnerability point. Still, a small percentage of virus encounters do occur via CD-ROMs and other removable media, typically when infected retail software is installed. Thin clients are predominantly deployed with no local removable drives such as CD-ROMs, diskettes, or hard drives.

[2] *ICSA Labs Virus Prevalence Survey 2002*
[3] *Enterprise Development Mgt. Issues 2003: Fall, © 2003 Evans Data Corp.*
[4] *This vulnerability is zero only if this component is not installed on the thin client device*
[5] *Other in this table represents unknown vectors and 3rd party/freeware software distribution*

Email/Office applications

With thin clients, users execute their email and office productivity applications on centralized servers and/or blade PCs. These applications and their associated data execute only on the server/blade. The user interface for these applications is rendered locally on the thin client through the Terminal Services Remote Desktop Protocol (RDP) or the Citrix® Independent Computing Architecture (ICA®) protocol. This means any virus or vulnerability introduced through your email/office or other remote applications typically affect the server/blade and not the thin client.

Additionally, the administrator has total control over the crucial applications and data on the servers or blade PCs, and can readily manage and deploy virus and firewall protection to these centralized systems. While these backend systems are at risk, applying patches or hot-fixes to centralized computing resources is more cost effective and takes less time than it does for standalone PC systems.

Web Browser/Internet/Non-email/Peer-to-Peer

These vectors and technologies are a growing concern. The majority of infection occurs through infected/malicious code that is downloaded or shared via these technologies. Security holes in internet browsers are reported frequently. Browser-related intrusions are centered on JavaScript, Java Applets and Active X.

The thin client model addresses these exposures in several ways. First, peer-to-peer applications and many of the internet and non-email web services are typically not deployed on thin clients. The best thin client strategy is to deploy only what you need to achieve your business goals. Second, user initiated file downloads and sharing typically occur at the server/blade PC level and not on the thin client itself. The thin client typically does not provide the user with the space and access rights to support this. For example, on HP XPe thin clients, the Enhanced Write Filter (EWF) prevents permanent modifications (writes) to the contents of the system's flash. Finally, the internet browser is an optional feature on the HP thin clients. It can be removed to ensure a more secure environment.

Operating System

Compared to a standard PC operating system, embedded operating systems are substantially smaller, providing less surface area to attack. Also, it is usually easier to configure an embedded OS to have fewer services that can be exploited than it is for a standard operating system. Advantages of the operating system will differ based upon the embedded OS chosen. Different operating systems are targeted at different rates and inherently have unique vulnerabilities. For example, CE .NET is substantially smaller and lighter than XPe or XP and is not targeted aggressively.

The following is a comparison of operating systems and their exposure on HP systems to the most exploited vulnerabilities of 2003 as listed by TruSecure®.[6] As compared to a standard Windows PC, only two (MS03-026 and MS03-007) or around 22% these nine most exploited vulnerabilities were relevant to the HP XPe thin client. Patches for both are included in the image.

Number of Viruses	Exploited Vulnerability Number	Exploited Vulnerability Name
28	MS01-020	Incorrect MIME Header Can Cause IE to Execute Email Attachment
16	MS00-072	Share Level Password
6	MS03-026	Buffer Overrun In RPC Interface Could Allow Code Execution
3	MS99-032	Scriptlet.typelib/eyedog
2	MS00-075	Microsoft VM ActiveX Component
1	MS99-042	IRFRAME ExecCommand
1	MS00-043	Malformed Email Header
1	MS00-046	Cache Bypass
1	MS03-007	Unchecked Buffer in Windows Component

In addition to being a smaller target, HP's thin client XP embedded OS contains an Enhanced Write Filter (EWF) preventing damage to the local file system and its OS files. The EWF protects the contents of the media by redirecting all the writes to a temporary virtual memory location. These writes are lost when the system is shutdown or restarted. Finally, none of these vulnerabilities were relevant to the HP CE .NET thin client. CE .NET is significantly smaller than XPe and is not a targeted operating system.

Instant Messaging

2003 saw a rise in viruses that infected devices via instant messenger (IM) clients. The proliferation of IM clients and greater acceptance of their use in corporate settings will continue to increase the attractiveness of this vulnerability for virus infections[6]. Instant messenger is an optional component for the HP thin client and can be removed to ensure the most secure environment.

Multimedia Viewers

This technology is a growing concern for security conscious network administrators. The majority of infection occurs through infected/malicious code that is downloaded or shared via the internet. Security holes in internet Media Player have also been reported. Media Player-related intrusions are centered on requests and downloads of media files and skins. Media Player is an optional component for the HP thin client and can be removed to ensure the most secure environment.

[6] *Wildtrends 2003: A Look at Virus Trends in 2003 and a Few Prediction for 2004; A TruSecure® Whitepaper*

Thin Client Firewall

Another key component to ensure the most secure computing environment is a firewall. HP offers the Microsoft Firewall as an add-on. If one of your systems on the network is compromised by malicious code, the firewall will prevent your thin client from infection. Additionally, a firewall will help prevent external attacks from reaching your system, protecting against intruders infecting the thin client with malicious code.

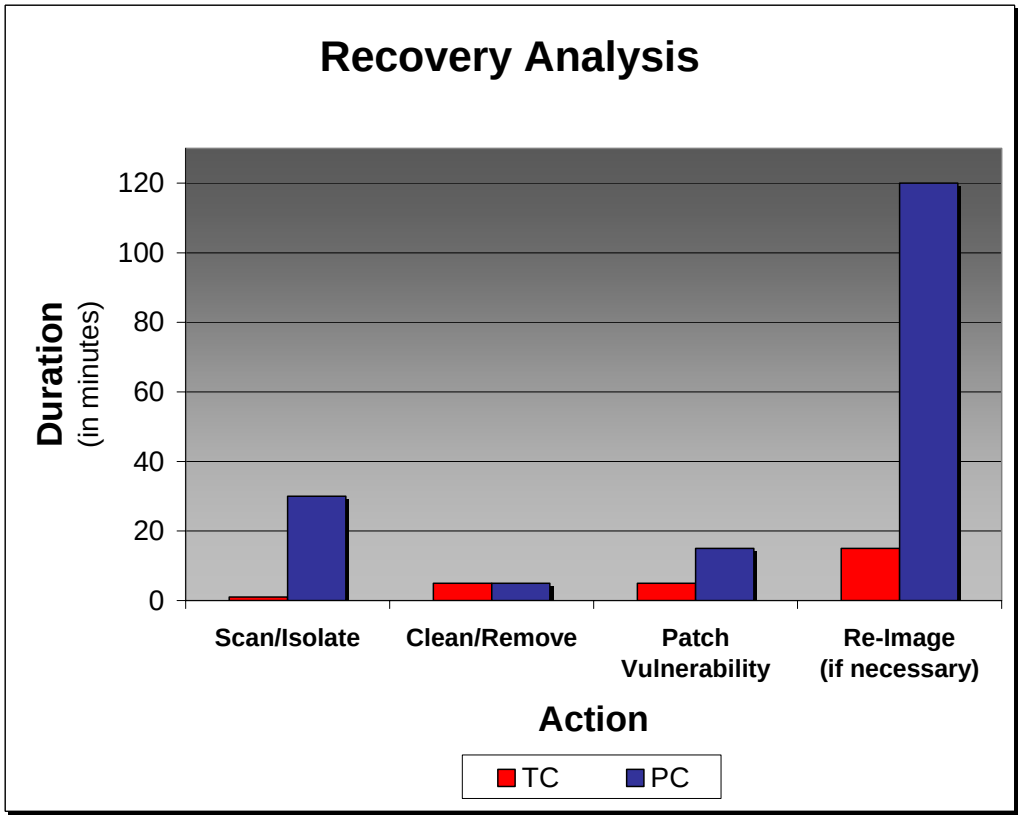
The Internet Connection Firewall can be downloaded at:

http://h18007.www1.hp.com/support/files/ThinClients/us/download/20070.html

Recovery Time

In the event of a virus attack or other security issue, the HP thin client computing model offers significantly shorter recovery time when compared to the traditional desktop model. If a thin client's image is compromised or corrupted , the recovery time is typically measured in minutes instead of hours. Recovery usually involves a power cycle (1 minute), patch (5 minutes), or re-image (15 minutes) of the system. This is substantially less time than the typical two hours it takes to re-image a PC or the multiple hours that can be spent rebuilding and recovering a user's data and environment.

The following graph compares the average recovery time of thin clients and desktop computers. In all categories, the HP thin client computing model meets or greatly exceeds the recovery speed performance of the traditional desktop computing model.



Summary

The HP thin client computing model provides significantly better virus protection than its PC counterpart. This protection is achieved by:

- Centralizing an enterprise's computer resources in the data center.
- Using centralized virus protection and firewall tools to protect these resources.
- Segregating the user's data for enhanced security, backup, and quick recovery.
- Deploying HP thin clients for simple, secure, reliable, and efficient access to these centralized resources.
- Using HP centralized management tools to manage and patch at all levels of the enterprise.

08/2004

P/N 367974-001